Approved: _____
MAGGIE LYNAUGH
Assistant United States Attorney

ORIGINAL

Before: THE HONORABLE DEBRA FREEMAN
United States Magistrate Judge
Southern District of New York

- - - - - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA :

- v. - :

ILYA LICHTENSTEIN, :

Defendant. :

- - - - - - - - - - - - - - - - - - - X

22 Mag. 1279

RULE 5(c)(3)
AFFIDAVIT

SOUTHERN DISTRICT OF NEW YORK, ss:

CHRISTOPHER JANCZEWSKI, being duly sworn, deposes and says that he is a Special Agent assigned to the Internal Revenue Service, Criminal Investigations, and charges as follows:

On or about February 7, 2022, the United States District Court for the District of Columbia issued a warrant for the arrest of "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)," based on a complaint charging "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" with one count of money laundering conspiracy, in violation of 18 U.S.C. § 1956(h), and one count of conspiracy to defraud the United States, in violation of 18 U.S.C. § 371. A copy of the arrest warrant and the complaint are attached as Exhibit A hereto and incorporated by reference herein.

I believe that ILYA LICHTENSTEIN, the defendant, who was arrested on or about February 8, 2022, in the Southern District of New York, is the same person as the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" who is wanted by the United States District Court for the District of Columbia.

The bases for my knowledge and for the foregoing charge are, in part, as follows:

1. I am a Special Agent assigned to the Internal Revenue Service, Criminal Investigations. I have been personally involved in determining whether ILYA LICHTENSTEIN, the defendant, is the same individual as the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" named in the February 7, 2022 arrest warrant from the United States District Court for the District of Columbia. Because this affidavit is being submitted for the limited purpose of establishing the identity of the defendant, I have not included in this affidavit each and every fact that I have learned. Where I report statements made by others, those statements are described in substance and in part, unless otherwise noted.

2. Based on my review of documents from proceedings in the United States District Court for the District of Columbia, I know that, on or about February 7, 2022, the United States District Court for the District of Columbia issued a warrant for the arrest of "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" (the "Arrest Warrant"). The Arrest Warrant was based on a complaint (the "Complaint") charging "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" with one count of money laundering conspiracy, in violation of 18 U.S.C. § 1956(h), and one count of conspiracy to defraud the United States, in violation of 18 U.S.C. § 371. The Complaint was issued in connection with case number 22-mj-00022 in the District of Columbia.

3. On or about February 8, 2022, at approximately 7:00 a.m., ILYA LICHTENSTEIN, the defendant, was arrested at his apartment in New York, New York.

4. At the time of arrest, ILYA LICHTENSTEIN, the defendant, had in his possession a driver's license issued by the state of New York bearing the name "Ilya Lichtenstein" and a date of birth of August 20, 1987, which matches the date of birth of the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" sought in the Arrest Warrant.

5. I have reviewed photographs of the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" sought in the Arrest Warrant, and I have determined that the appearance of the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" sought in the Arrest Warrant matches both the appearance of ILYA LICHTENSTEIN,

the defendant, and the photograph on the driver's license in LICHTENSTEIN's possession.

6. Based on the fact that ILYA LICHTENSTEIN, the defendant, possessed identification bearing the name and date of birth of "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)", and that the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" sought in the Arrest Warrant matches the appearance of LICHTENSTEIN and the photograph on LICHTENSTEIN's driver's license, I believe that LICHTENSTEIN is the "Ilya Lichtenstein (AKA: Ilya 'Dutch' Lichtenstein, Ilya Likhtenshteyn)" sought in the Arrest Warrant.

WHEREFORE, I respectfully request that ILYA LICHTENSTEIN, the defendant, be imprisoned or bailed as the case may be.

CHRISTOPHER JANCZEWSKI
SPECIAL AGENT
INTERNAL REVENUE SERVICE
CRIMINAL INVESTIGATION

Sworn to before me this,
8th day of February, 2022

THE HONORABLE DEBRA FREEMAN
United States Magistrate Judge
Southern District of New York

EXHIBIT A

This second page contains personal identifiers provided for law-enforcement use only and therefore should not be filed in court with the executed warrant unless under seal.

(Not for Public Disclosure)

Name of defendant/offender: Ilya Lichtenstein

Known aliases: Ilya "Dutch" Lichtenstein, Ilya Likhtenshteyn

Last known residence: 75 Wall St, 33M, New York, NY 10005

Prior addresses to which defendant/offender may still have ties: n/a

n/a

Last known employment: self-employed via Endpass, Inc and Demandpath LLC

Last known telephone numbers: 847-208-2167

Place of birth: Rostov, Russia

Date of birth: 8/20/1987

Social Security number: 324-90-3212

Height: 5'08" Weight: 125

Sex: Male Race: white

Hair: black Eyes: green

Scars, tattoos, other distinguishing marks: unknown

unknown

History of violence, weapons, drug use: unknown

unknown

Known family, friends, and other associates *(name, relation, address, phone number)*:

FBI number:

Complete description of auto:

Investigative agency: IRS-CI; FBI; HSI

Investigative agency address: 1200 1st St NE Room 4300, Washington, DC 20002

Name and telephone numbers (office and cell) of pretrial services or probation officer *(if applicable)*:

Date of last contact with pretrial services or probation officer *(if applicable)*:

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
Ilya Lichtenstein (AKA: Ilya "Dutch" Lichtenstein, Ilya Likhtenshteyn) (DOB: 08/20/1987), and
Heather Rhiannon Morgan (AKA: Razzlekhan) (DOB: 05/28/1990)

Defendant(s)

Case: 1:22-mj-00022
Assigned to: Judge Meriweather, Robin M.
Assign Date: 2/7/2022
Description: COMPLAINT W/ ARREST WARRANT

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 2016 to February 2022 in the county of _____ in the _____ in the District of Columbia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1956(h)	(Money Laundering Conspiracy)
18 U.S.C. § 371	(Conspiracy To Defraud the United States)

This criminal complaint is based on these facts:

See attached statement of facts.

☒ Continued on the attached sheet.

Complainant's signature

Christopher Janczewski, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 02/07/2022

Robin M. Meriweather 2022.02.07 11:09:24 -05'00'

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather, U.S. Magistrate Judge
Printed name and title

Case: 1:22-mj-00022
Assigned to: Judge Meriweather, Robin M.
Assign Date: 2/7/2022
Description: COMPLAINT W/ ARREST WARRANT

STATEMENT OF FACTS

1. Your affiant, Christopher Janczewski, is a Special Agent assigned to the Internal Revenue Service, Criminal Investigation (IRS-CI). As a Special Agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code, Sections 1956 and 1957), the Bank Secrecy Act (including relevant parts of Title 31, United States Code), and related offenses. I have experience investigating crimes involving virtual currency,[1] as further described below. I also am experienced in analyzing and tracing virtual currency transactions. Currently, I am tasked with investigating the laundering of funds stolen from a virtual currency exchange ("Victim VCE") in 2016. As a Special Agent, I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws.

2. The facts and information contained in this Affidavit are based on my personal knowledge and observations, information provided to me by others,[2] and a review of documents and records. This Affidavit does not contain each and every fact known to the Government. It contains only those facts I believe are sufficient to support a finding of probable cause that ILYA "DUTCH" LICHTENSTEIN, a citizen of Russia and the United States, and his wife, HEATHER MORGAN, a citizen of the United States, committed the following offenses: Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); and Conspiracy to Defraud the United States, in violation of 18 U.S.C. § 371.

I. Introduction

3. IRS-CI, the Federal Bureau of Investigation (FBI), and Homeland Security Investigations (HSI) have been investigating the theft of funds from a well-known virtual currency exchange[3] ("Victim VCE") that was hacked in 2016. Victim VCE is one of the world's largest virtual currency exchanges and allows customers to buy, sell, and store various types of virtual currency.

---

[1] Virtual currency is a digital form of value that is circulated over the Internet and is not backed by a government. Bitcoin (BTC) is one of the most popular forms of virtual currency.

[2] The information contained in this affidavit includes information provided by private entities that the U.S. Government believes to be reliable. In August 2020, Victim VCE announced a sizable reward related to the return of the stolen funds. Specifically, Victim VCE offered up to 5% of any property recovered. The total potential reward money exceeds $400 million. The U.S. Government understands that Victim VCE has indicated that some portion of the reward could be made available even where the information provided indirectly leads to the recovery of funds (*e.g.*, where a company provides information to the U.S. Government, that is then able to locate and restrain the funds based on that information). Entities who provided information to the U.S. Government in this matter may therefore be financially motivated. The U.S. Government vetted any leads as appropriate, with consideration given to the potential financial motivation. The U.S. Government is not a party to any agreement between Victim VCE and private individuals or entities and has not been a part of discussions regarding potential rewards.

[3] A virtual currency exchange ("VCE") is a business that allows customers to buy, sell, or trade virtual currency. Many VCEs also store virtual currency on behalf of their customers. VCEs doing business in the United States are regulated by the U.S. Department of Treasury and are required to establish anti-money laundering (AML) programs—that is, controls designed to detect and deter money laundering.

4. In or around August 2016, a hacker breached Victim VCE's security systems and infiltrated its infrastructure. While inside Victim VCE's network, the hacker was able to initiate over 2,000 unauthorized BTC transactions, in which approximately 119,754 BTC was transferred from Victim VCE's wallets[4] to an outside wallet (Wallet 1CGA4s[5]). At the time of the breach, 119,754 BTC was valued at approximately $71 million. Due to the increase in the value[6] of BTC since the breach, the stolen funds are valued at over $4.5 billion as of February 2022.

5. U.S. authorities traced the stolen funds on the BTC blockchain.[7] As detailed below, beginning in or around January 2017, a portion of the stolen BTC moved out of Wallet 1CGA4s in a series of small, complex transactions across multiple accounts and platforms. This shuffling, which created a voluminous number of transactions, appeared to be designed to conceal the path of the stolen BTC, making it difficult for law enforcement to trace the funds. Despite these efforts, as explained further below, U.S. authorities traced the stolen BTC to multiple accounts controlled by ILYA "DUTCH" LICHTENSTEIN, a Russian-U.S. national residing in New York, and his wife HEATHER MORGAN.

6. The 2017 transfers notwithstanding, the majority of the stolen funds remained in Wallet 1CGA4s from August 2016 until January 31, 2022. On January 31, 2022, law enforcement gained access to Wallet 1CGA4s by decrypting a file saved to LICHTENSTEIN's cloud storage account,[8] which had been obtained pursuant to a search warrant. The file contained a list of 2,000 virtual currency addresses, along with corresponding private keys.[9] Blockchain analysis confirmed that almost all[10] of those addresses were directly linked to the hack. Between January 31, 2022, and February 1, 2022, law enforcement obtained approval to execute a lawful seizure supported by probable cause under exigent circumstances and used the private keys from LICHTENSTEIN's file to seize Wallet 1CGA4's remaining balance of approximately 94,636 BTC, worth $3.629 billion. On February 2, 2022, the government requested, and on February 4, 2022, a court issued a seizure warrant authorizing the seizure of those funds. Those funds remain secured in the U.S. Government's possession.

---

[4] The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets are used to store and transact in virtual currency. A wallet may include many virtual currency addresses, roughly equivalent to anonymous account numbers.

[5] BTC wallets and clusters in this affidavit will be referred to by the first six characters of the BTC address associated with the wallet or cluster.

[6] The trading value of BTC fluctuates over time, depending on market demand.

[7] The BTC blockchain is a public transaction ledger that includes a record of every BTC transaction that has ever occurred.

[8] A cloud storage account allows users to store computer files in a remote location, rather than saved to their own devices.

[9] Each virtual currency address has a corresponding private key, which is roughly equivalent to a complex password or PIN code and which is needed to spend any virtual currency contained in the address.

[10] More specifically, all of the 2,000 addresses either contained BTC directly linked to the hack of Victim VCE (*i.e.*, was exclusively funded from the hack) or did not contain any virtual currency at all (*i.e.*, they contained a balance of zero and had never been used to transact in virtual currency).

II. Tracing the Stolen BTC to LICHTENSTEIN and MORGAN

A. Summary

7. During the investigation, and as further described below, special agents traced the stolen funds as follows:

a. **First**, to Wallet 1CGa4s, an unhosted wallet[11] containing over 2,000 BTC addresses (which were saved, along with their associated private keys, in LICHTENSTEIN's cloud storage account), where the stolen funds remained dormant until January 2017;

b. **Second**, to accounts at the darknet market AlphaBay;[12]

c. **Third**, to seven interconnected accounts at a U.S.-based VCE ("VCE 1"), as well as accounts at additional VCEs ("VCE 2," "VCE 3," and "VCE 4");

d. **Fourth**, to various unhosted BTC wallets; and

e. **Fifth**, to accounts owned by LICHTENSTEIN and MORGAN at six other VCEs ("VCE 5," "VCE 6," "VCE 7," "VCE 8," "VCE 9," and "VCE 10").

Close financial analysis and other evidence revealed that all of the above laundering activity was conducted by LICHTENSTEIN and MORGAN.

8. In conducting these transactions, and as described further below, LICHTENSTEIN and MORGAN employed numerous money laundering techniques, including: (1) using accounts set up with fictitious identities; (2) moving the stolen funds in a series of small amounts, totaling thousands of transactions, as opposed to moving the funds all at once or in larger chunks; (3) utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; (4) layering the stolen funds by depositing them into accounts at a variety of VCEs and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; (5) converting the BTC to other forms of virtual currency, including anonymity-enhanced virtual currency,[13] in a practice known as "chain hopping"; and (6) using U.S.-based business accounts to legitimize activity.

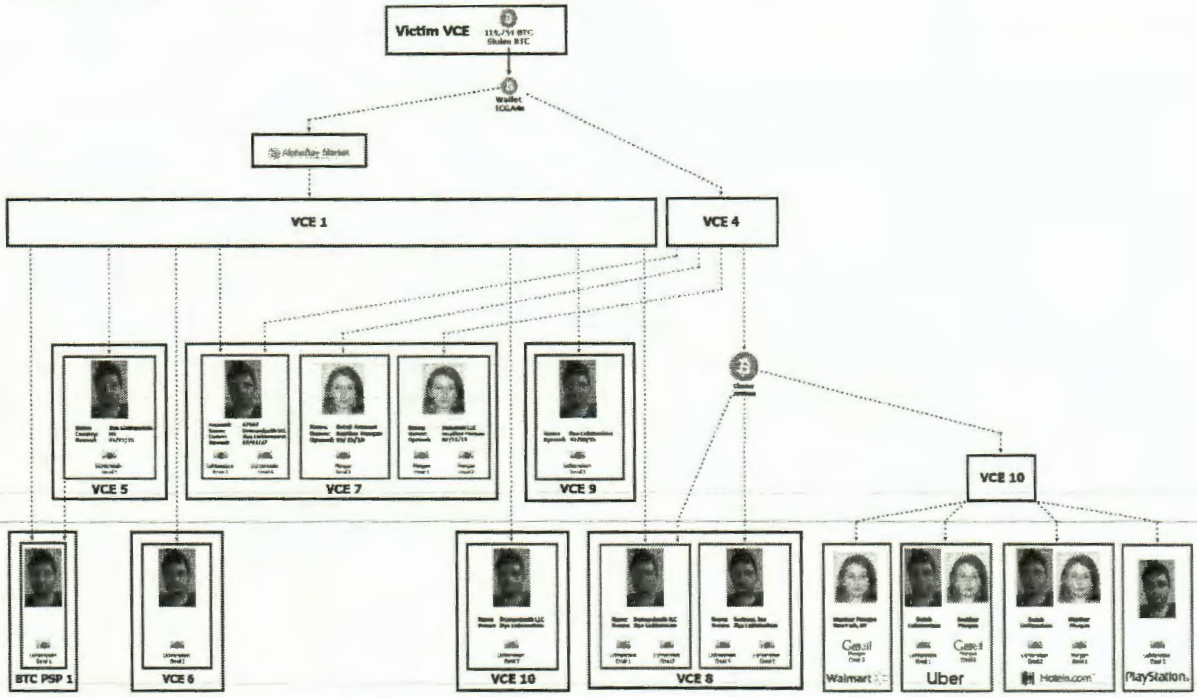
---

[11] BTC wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are called "unhosted" wallets.

[12] A darknet market is an ecommerce platform through which vendors can sell illegal goods and services, such as illegal narcotics, stolen financial information, and hacking tools. Darknet markets typically allow users to create accounts and deposit, store, and withdraw virtual currency from those accounts, in order to buy and sell items on the site. AlphaBay was one of the largest darknet markets and operated from December 2014 through July 2017.

[13] Anonymity-enhanced virtual currency, also called anonymity-enhanced cryptocurrency (AECs) or privacy coins, are virtual currency alternatives to BTC which endeavor to provide greater anonymity when making transactions.

9. The chart[14] below is a simplified[15] illustration of how the stolen BTC moved in a series of transactions from Victim VCE to accounts connected to LICHTENSTEIN and MORGAN:



10. As summarized in the above chart, law enforcement traced the stolen funds through thousands of transactions to over a dozen accounts in the true name of LICHTENSTEIN, MORGAN, and/or their businesses. Law enforcement was also able to determine that numerous accounts set up with fictitious personas and involved in the laundering were, in fact, controlled by LICHTENSTEIN and MORGAN. Several key examples of this tracing—but by no means every example—are included in the subsequent subsections.

[14] Charts within this affidavit that display the symbol of an orange circle with a "B" and two lines running vertically through that "B" is a representation of BTC. The symbol of an orange and grey circle with a white M running through it is a representation of Monero (XMR), an anonymity-focused virtual currency discussed later in this complaint.

[15] Because the stolen BTC was transferred and split up so many times, condensing all the transaction information into one chart would be impractical. The charts within this affidavit do not depict all known transactions, or even all transactions related to the activity depicted. Rather, they are meant to be illustrations of the general flow of the stolen BTC from one point to another.

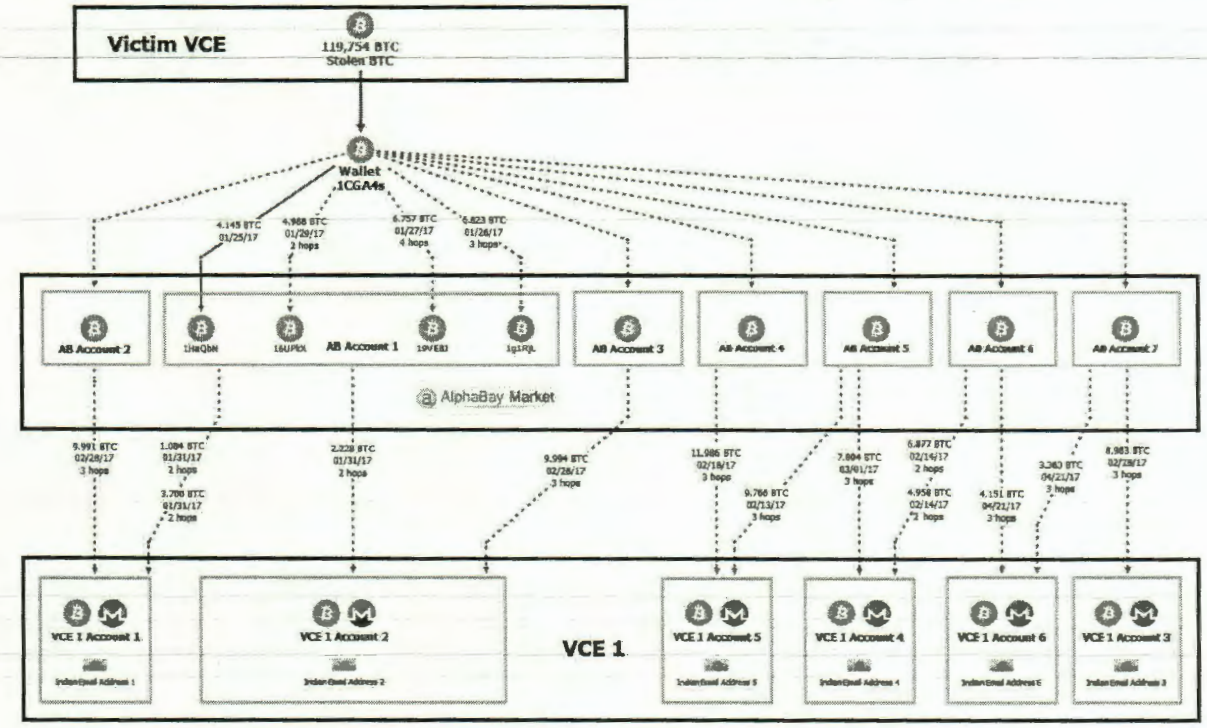
B. AlphaBay Pass-Through Activity

11. The early movement of the stolen funds involved extensive layering activity that employed the peel chain technique.[16] As part of this layering, a portion of the stolen funds were deposited gradually (an indication of peel chain activity) into AlphaBay accounts.

12. The AlphaBay accounts were used as a pass-through for the stolen BTC. Depositing and withdrawing BTC at AlphaBay allowed LICHTENSTEIN and MORGAN to break up the stolen BTC trail on the blockchain. After being moved into accounts at AlphaBay, the stolen BTC was withdrawn, layered, and ultimately deposited into VCEs around the world, as described in pertinent part immediately below.

C. Tracing the Stolen funds through AlphaBay to VCE 1, 2, 3, and 4

13. The chart below shows part of the movement of the stolen funds from Victim VCE to AlphaBay (abbreviated "AB" in some places), and then from AlphaBay to VCE 1:[17]



[16] A "peel chain" occurs when a large amount of BTC sitting at one address is sent through a series of transactions in which a slightly smaller amount of BTC is transferred to a new address each time. In each transaction, some quantity of BTC "peel off" the chain to another address (frequently, to be deposited into a VCE), and the remaining balance is transferred to the next address in the chain. In my training and experience, I know that it is common for money launderers to rely on a peel chain to obstruct the movement of the illicit money.

[17] As previously stated, showing all of the hops and connections between accounts in a single chart would make these charts very difficult to read. Throughout this affidavit, each chart is used to highlight pertinent transactions for the purpose of showing the flow of funds and establishing probable cause.

14. As depicted in the chart above, a portion of funds laundered through AlphaBay were sent to six VCE 1 accounts ("VCE 1 Account 1" through "VCE 1 Account 6"). Records from VCE 1 showed that these six accounts were all registered using email addresses hosted by the same India-based email provider. Those records also showed that there were two other similar accounts at VCE 1 registered using an email address from that same India-based provider: "VCE 1 Account 7" and "VCE 1 Account 8."

15. The relevant VCE 1 accounts were registered in the names of third parties unrelated to LICHTENSTEIN and MORGAN. VCE 1 was unable to verify the identities of any of the listed account owners. Specifically, in February and March 2017, VCE 1's employees requested that the registered accountholders for seven of the accounts provide additional identifying information to verify their account ownership. VCE 1 did not receive a response to these requests. As a result, VCE 1 froze[18] the accounts. In total, the accounts contained over $186,000 U.S. dollars' worth of virtual currency at the time, in or around April 2017.[19]

16. The above-referenced eight VCE 1 accounts shared notable commonalities leading investigators to believe that they were owned by the same individual. Specifically, overlapping subsets of the accounts: (1) were tied to similarly styled email addresses hosted by the same India-based provider; (2) were accessed by the same IP addresses; (3) were created around the same time period surrounding the hack of Victim VCE in or around August 2016; (4) were engaged in similar trading patterns entailing chain hopping[20] to anonymity-enhanced virtual currency; and/or (5) were abandoned following a request for additional know-your-customer (KYC)[21] information. The connection among the VCE 1 accounts was further confirmed upon reviewing a spreadsheet saved to LICHTENSTEIN's cloud storage account. The spreadsheet included the log-in information for accounts at various virtual currency exchanges and a notation regarding the status of the accounts. Six of the VCE 1 accounts referenced above were included in the spreadsheet, with a notation indicating "FROZEN." In other words, LICHTENSTEIN possessed a document with the login information for the accounts at VCE 1 that received funds traceable to the hack of Victim VCE and that reflected his knowledge that the accounts had been frozen.

17. Further blockchain analysis revealed that stolen funds moved through AlphaBay were also sent to accounts at a foreign VCE ("VCE 2") and a U.S.-based VCE ("VCE 4"). Those accounts were registered using an email address associated with the above-referenced India-based email provider. The log-in details for those accounts at VCE 2 and VCE 4, including the VCE's name and the email address hosted by the India-based provider, were included in the spreadsheet found in LICHTENSTEIN's cloud storage account.

---

[18] As part of their anti-money laundering practices, financial institutions may "freeze" funds or accounts—that is, disable withdrawals—where they suspect the accounts are being used for illegal activity.

[19] The funds contained within VCE 1 Accounts 1 through 8 (excluding VCE 1 Account 6) have been seized by law enforcement pursuant to a separate investigation.

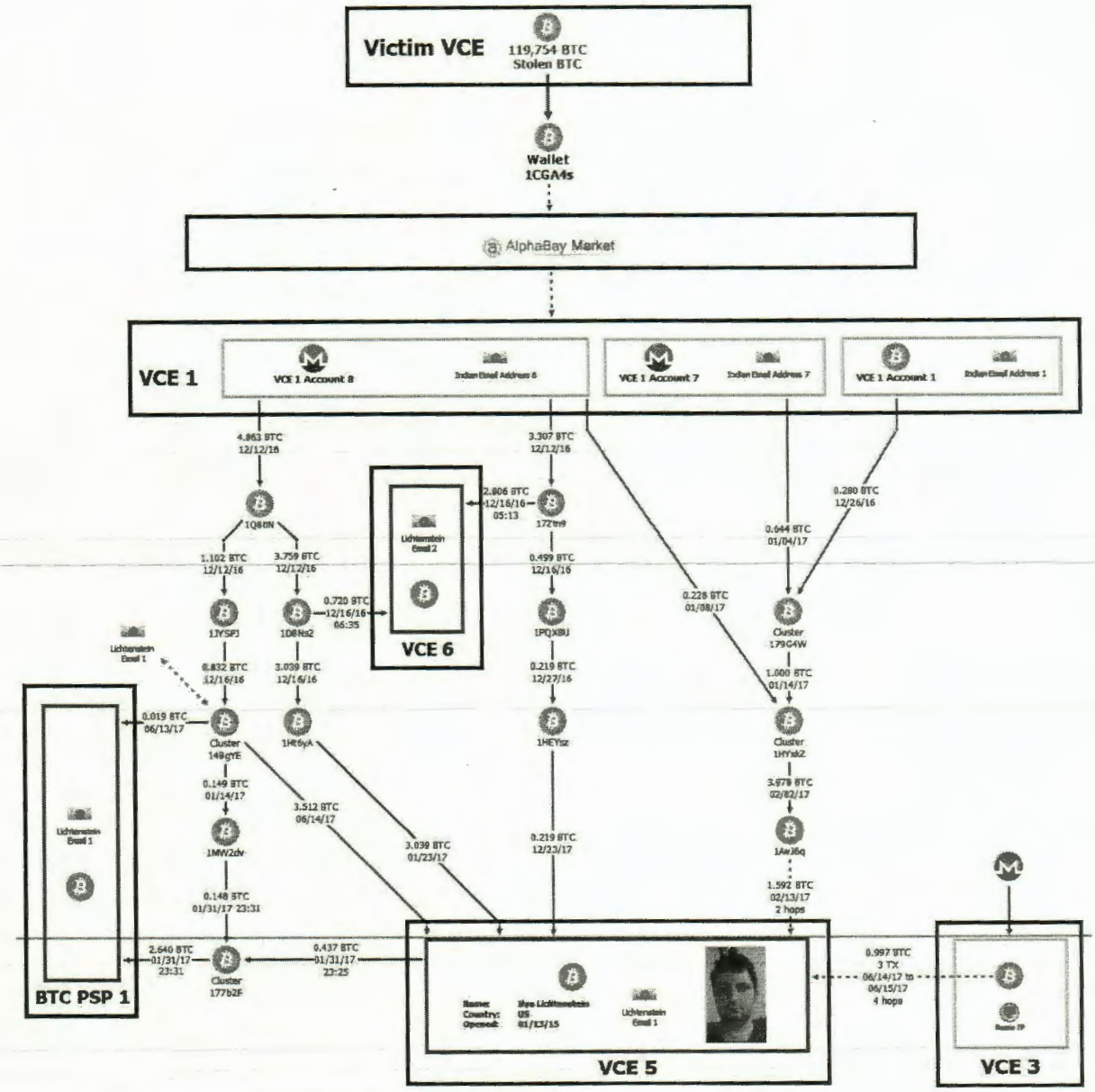
[20] Chain-hopping is a money laundering technique involving converting one form of virtual currency to another, making the transaction paths more difficult to track.

[21] Know-your-customer (KYC) information is information about customers and their activities that financial institutions collect as part of their AML procedures.

18. The account at VCE 2 converted BTC to Dash, another form of virtual currency. Shortly thereafter, two accounts at VCE 4 received Dash deposits. Those VCE 4 accounts were registered to emails contained in the account spreadsheet located on LICHTENSTEIN's cloud storage account.

D. Following the Stolen Funds to an Account at VCE 5 in the Name Ilya LICHTENSTEIN

19. Special agents continued to trace the stolen funds moved through VCE 1 prior to the accounts being frozen by VCE 1. The funds were sent to various locations, including through multiple unhosted BTC addresses to an account at another U.S.-based VCE ("VCE 5") in LICHTENSTEIN's name ("Lichtenstein's VCE 5 Account"). As illustrated below, the withdrawals from multiple VCE 1 accounts merge together as they flow through a peel chain and ultimately fund a deposit on or about February 13, 2017, to Lichtenstein's VCE 5 account (as well as other deposits in January, June, and December 2017):



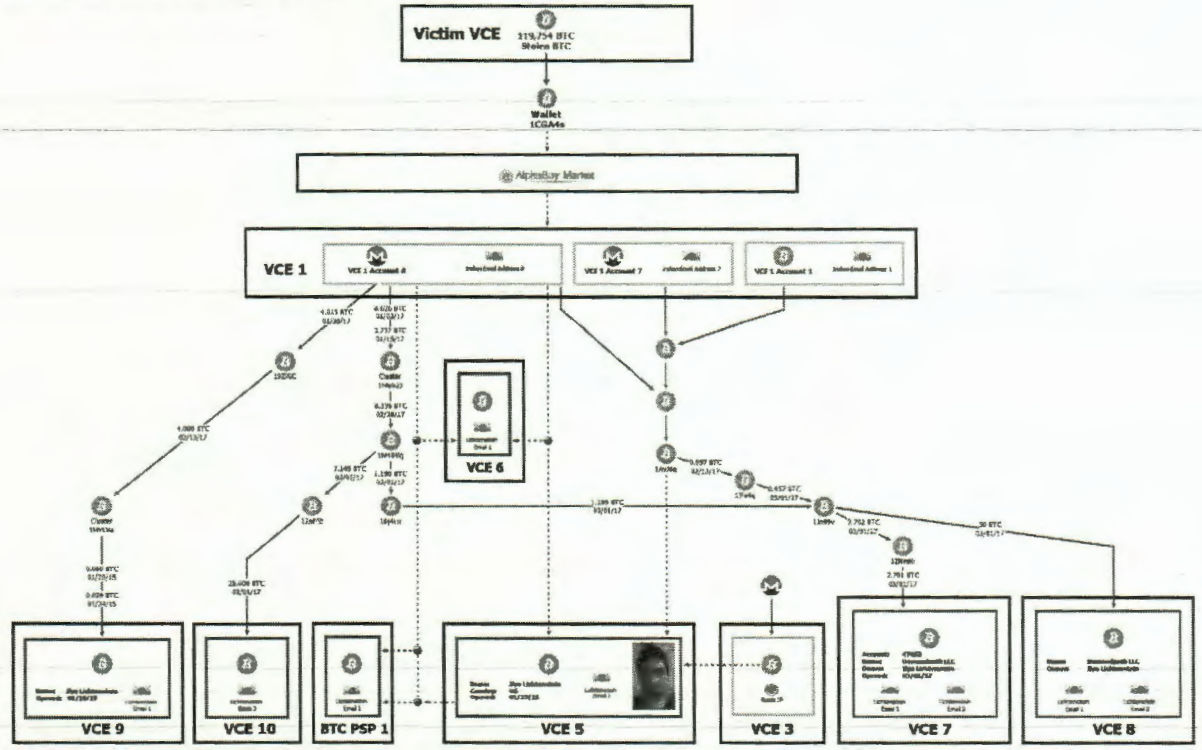
20. Records from VCE 5 showed that Lichtenstein's VCE 5 Account was opened on or about January 13, 2015, in his name and using his address at the time in San Francisco. The account was verified with photographs of LICHTENSTEIN's California driver's license and a selfie-style photograph. The account was registered to an email address containing LICHTENSTEIN's first name ("Lichtenstein Email 1"). Search warrants for the contents of the Lichtenstein Email 1 account confirmed that LICHTENSTEIN controlled the account, as well as a related account which included LICHTENSTEIN's nickname ("Lichtenstein Email 2").

21. Lichtenstein's VCE 5 Account was used to purchase gold from a precious metals dealer through a U.S.-based virtual currency payment service provider ("BTC PSP 1").[22] In conducting the transaction, LICHTENSTEIN provided his true home address for shipment.

E. Tracing the Stolen Funds to LICHTENSTEIN and MORGAN's Accounts at Additional VCEs

i. Overview of LICHTENSTEIN's Activity

22. Additional funds traced to the Victim VCE theft were also sent to LICHTENSTEIN's accounts at five more VCEs: "VCE 6," "VCE 7," "VCE 8," "VCE 9," and "VCE 10." Specifically, the chart below shows that a portion of the stolen funds flowed from VCE 1 Account 1, VCE 1 Account 7, and VCE 1 Account 8, through multiple transactions into accounts at VCE 7, VCE 8, VCE 9, and VCE 10:



23. Records obtained from the various VCEs showed that the accounts were opened in LICHTENSTEIN's name and/or the name of LICHTENSTEIN's businesses. Many of the accounts were verified with additional information and/or identification documents provided by LICHTENSTEIN. For example, in a KYC verification email from VCE 10 in 2019, LICHTENSTEIN wrote to representatives from VCE 10 that he has "been investing in and mining [BTC] since 2013, so the source of funds would be those early crypto assets."

[22] BTC PSP 1 is a VCE service that accepts virtual currency on behalf of a merchant and then remits payment to the merchant in fiat currency, such as the U.S. dollar. This allows a merchant to offer BTC as a means of payment for customers without requiring the merchant itself to handle the BTC.

24. Between the 2016 hack and the present, LICHTENSTEIN and MORGAN further engaged in a diverse array of virtual currency transactions, including transacting in numerous altcoins, liquidating BTC through a BTC ATM,[23] and purchasing non-fungible tokens (NFTs).[24]

ii. The Flow of Funds from Accounts at VCE 4 to LICHTENSTEIN and MORGAN

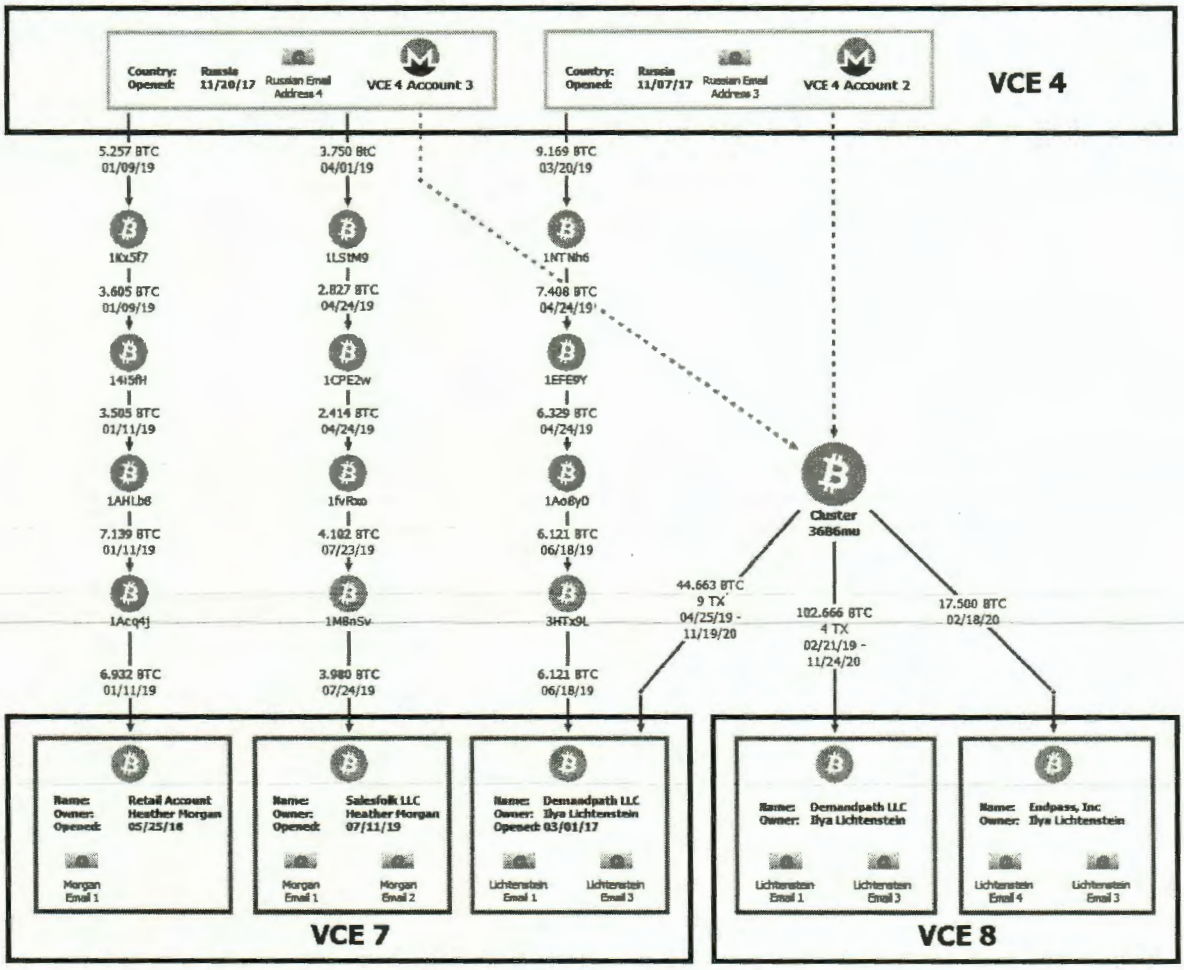
25. After scrutinizing the above-referenced flow of stolen funds into the multiple accounts connected to LICHTENSTEIN at VCE 5, VCE 6, VCE 7, VCE 8, VCE 9, and VCE 10, investigators analyzed (via publicly available information on the BTC blockchain and records obtained from the VCEs) all of the transactions into each of LICHTENSTEIN's accounts, and discovered the following:

a. A large portion of BTC deposited into LICHTENSTEIN's VCE accounts was traced back to two accounts at VCE 4. These accounts are referenced below as "VCE 4 Account 2" and "VCE 4 Account 3."

b. These two accounts at VCE 4, as depicted below, also sent funds into accounts registered to MORGAN and into another account registered to a business owned by LICHTENSTEIN called Endpass, Inc. ("Endpass").

[23] Bitcoin Automated Teller Machines (ATMs)—also called BTMs, convertible virtual currency kiosks or crypto ATMs—are ATM-like devices or electronic terminals that allow users to exchange cash and virtual currency. BTC ATMs are types of VCEs and are regulated by FinCEN.

[24] Non-fungible tokens (NFTs) are blockchain-based digital units used to transfer or validate ownership of unique items, such as artwork.



26. Records from VCE 4 showed that VCE 4 Account 2 was created on or about November 7, 2017, and was registered in the name of a Russian national and under a Russian email address. VCE 4 Account 2 was entirely funded by approximately 13,200 XMR,[25] via approximately 21 transactions that took place between in or around November 2017 and March 2019.

27. Another account at VCE 4 ("VCE 4 Account 3") was created on or about November 20, 2017, and was registered in the name of another Russian national and under another Russian email address. VCE 4 Account 3 was entirely funded by approximately 6,870 XMR, via approximately 10 transactions that took place between in or around November 2017 and April 2019.

[25] Monero (XMR) is a virtual currency designed to increase users' anonymity.

28. When employees from VCE 4 attempted (via email) to verify the identity of the individual listed as the owner of VCE 4 Account 2, the account owner represented to employees from VCE 4 that the source of funds was the owner's investments. Employees from VCE 4 followed up with the owner of VCE 4 Account 2 and asked the owner to provide a bank or investment statement to support that the source of funds within the account was from the owner's investments. The owner did not respond and never contacted VCE 4 again. As a result, VCE 4 froze VCE 4 Account 2. In the end, the owner of VCE 4 Account 2 abandoned the account with approximately $155,000 worth of virtual currency in it.

29. When employees from VCE 4 attempted to verify the identity of the individual named on the account for VCE 4 Account 3, the owner never responded. VCE 4 froze that account. It had no balance at the time, as all of the funds had been withdrawn previously.

30. The XMR deposited into VCE 4 Account 2 and VCE 4 Account 3 was all converted to BTC and then withdrawn, consistent with chain hopping. The same method was used to liquidate the funds from the VCE 1 accounts as described above.

iii. Deposits into MORGAN's Accounts at VCE 7

31. According to records provided by VCE 7 (and as illustrated above in paragraph 25), VCE 4 Account 3 deposited BTC into two accounts owned by MORGAN: one account in MORGAN's name ("Morgan's VCE 7 Account") and one in the name of her company, SalesFolk LLC ("SalesFolk") ("Morgan's SalesFolk VCE 7 Account"). MORGAN responded to VCE 7's requests for KYC verification by using SalesFolk email addresses in MORGAN's name (Morgan Email 1) and initials (Morgan Email 2). In those communications, MORGAN sent SalesFolk's incorporation documents and advised VCE 7 that she was the sole owner of SalesFolk. Records from VCE 7 also indicated that another email address containing MORGAN's name (Morgan Email 3) was connected to the two accounts under MORGAN's name and company details at VCE 7.

32. As described in more detail below, MORGAN advised representatives from VCE 7 that SalesFolk accepted BTC as payment from customers. However, special agents were unable to corroborate MORGAN's statement with any actual payment details or publicly available information about SalesFolk's acceptance of BTC as payment, with one exception, an account in SalesFolk's name at BTC PSP 1. That account received approximately $130,000 worth of virtual currency from a single company ("Shell Company 1"), which claimed to operate out of Hong Kong. The payment was purportedly for advertising services. However, Shell Company 1 had no website, and investigators were unable to identify any legitimate business activity by Shell Company 1, much less any advertising.

iv. LICHTENSTEIN and MORGAN's Misrepresentations to VCE 7

33. According to the records provided by VCE 7, LICHTENSTEIN's VCE 7 Account and MORGAN's two VCE 7 accounts (Lichtenstein's VCE 7 Account, Morgan's VCE 7 Account, and Morgan's SalesFolk VCE 7 Account) shared logins from the same IP addresses that

investigators geo-located to New York. In total, their three accounts at VCE 7 received around $2.9 million worth of BTC for the approximate period of March 1, 2017, to October 24, 2021, all after the hack of Victim VCE. Nearly all of the BTC received was converted to fiat currency and withdrawn to U.S. financial institution (USFI)[26] accounts held by MORGAN and LICHTENSTEIN. Business records show that the three primary financial accounts used by MORGAN to receive fiat currency that had been converted from BTC were all opened after the hack of Victim VCE.

34. Records from VCE 7 also showed that MORGAN and LICHTENSTEIN both provided false information to VCE 7 in relation to their accounts. More specifically, as part of VCE 7's AML/KYC policies, employees from VCE 7 asked LICHTENSTEIN various questions about his source of funds, his business, and the nature of his account at VCE 7 (Lichtenstein's VCE 7 Account). According to records provided by VCE 7, LICHTENSTEIN represented via email to VCE 7 that he would be using his VCE 7 account to trade only his own virtual currency that he had acquired as a result of his early investment in BTC. Specifically, on February 27, 2017, LICHTENSTEIN wrote the following to representatives from VCE 7: "Hi, I'm a tech entrepreneur and [BTC] early adopter since acquiring my first BTC in 2011. I'm looking to diversify a bit ahead of the ETF decision and sell about 100BTC. Please let me know the next steps to move forward. All trades I would execute are from my own personal funds, the LLC is simply there to manage my trading assets."

35. As noted above, according to the public blockchain and records obtained from VCEs, the primary source of funding for LICHTENSTEIN's VCE 7 account came from the aforementioned VCE 4 accounts (*i.e.*, the VCE accounts tied to Russian identity documents), opened after the hack of Victim VCE, not from early investment earnings.

36. In response to a VCE 7 representative's request for additional information about his company Demandpath LLC, LICHTENSTEIN stated that Demandpath LLC was a "simple single-member LLC," and so it did not have "articles of incorporation or a board of directors." LICHTENSTEIN also stated that he was the "sole beneficiary with 100% ownership."

37. As noted above, MORGAN had two accounts at VCE 7: a retail account and an institutional account. MORGAN represented via email to VCE 7 that she would be using her accounts at VCE 7 to receive funds from her business clients and also to transact with her own virtual currency. MORGAN claimed that the source of digital assets that would be deposited in her institutional account would be virtual currency that she had received in 2014 and 2015 from LICHTENSTEIN. This claim is belied by the blockchain, which shows that her virtual currency accounts received the bulk of deposits from the above-referenced accounts at VCE 4 and received none from identifiable business clients. This fraud is documented as follows:

a. On August 28, 2018, MORGAN reached out to VCE 7 representatives in regard to her retail account, asking for a limit increase (*i.e.*, she wanted to transact in higher

[26] Though VCEs are financial institutions under the Bank Secrecy Act, USFI is used in this affidavit to refer to non-VCE financial institutions, such as banks.

volume and was being blocked from doing so). MORGAN stated, "I tried to do a withdrawal for $8000 to my bank account that I sold in order to pay some upcoming bills, and was told that I could only transfer $500 a day via ACH or $15,000/month via wire."

b. Then, in or around June 2019, MORGAN applied for her institutional account. On June 27, 2019, a representative from VCE 7 reached out to MORGAN for information about how her business (SalesFolk) interacts with virtual currency and how her new institutional account would be used. MORGAN responded: "SalesFolk has some B2B customers that pay with cryptocurrency. Additionally, I also have some personal cryptocurrency of my own that I would like to sell to finance the development of some new software that we are beginning to build. Because the company is an LLC taxed as an S corp it has pass-through taxation and I am the sole owner. I was going to use some of my personal crypto to fund out new software projects."

c. On July 1, 2019, MORGAN stated that SalesFolk was not a financial institution, and so she does not manage her customers' money in any way. "[SalesFolk's customers are] just B2B companies buying software and/or sales/email marketing consulting services from us, typically around $8500 or less per contract/invoice, so we haven't been doing any KYC on them."

d. On July 2, 2019, a representative from VCE 7 asked MORGAN some follow-up questions about how MORGAN came to own the digital assets that would be deposited into her new institutional account. Morgan stated, "My boyfriend (now husband) gifted me cryptocurrency over several years (2014, 2015,), [sic] which have appreciated. I have been keeping them in cold storage."

e. On January 15, 2020, a representative from VCE 7 reached out to MORGAN for monthly funding amounts, trading volume, and transactional activity for the account going forward. MORGAN replied that she anticipated that monthly funding activity would be approximately "10-30K USD" and the trading volume would be "10-20k on average."

f. As previously stated, although MORGAN advised representatives from VCE 7 that SalesFolk received virtual currency from some of her customers, investigators were not able to locate anything on the SalesFolk website referencing accepting or dealing with cryptocurrency. While it is possible that SalesFolk received virtual currency, based on my experience, companies that do offer virtual currency as a payment method or in conjunction with another service often advertise it to attract more business. To date, investigators have not identified any evidence that SalesFolk in fact received any such virtual currency payments from purported SalesFolks customers, other than the payments from Shell Company 1 discussed above. Based on my training and experience, it appears that MORGAN actually switched her VCE 7 account to a business account from a personal account in order

to receive less scrutiny from VCE 7 about her transactions as she liquidated her BTC in greater volume.

38. In sum, MORGAN and LICHTENSTEIN each advised VCE 7 that the source of the BTC deposited into their accounts came from their own investments dating to before 2015. However, detailed blockchain analysis, as illustrated in part above, revealed that the primary source of the BTC was the VCE 4 accounts that were opened in 2017 after the hack. These facts contradict MORGAN's and LICHTENSTEIN's representations to VCE 7 about the source of the funds.

39. Records obtained from other VCEs and traditional financial institutions revealed that MORGAN and LICHTENSTEIN made similar deceptive statements to other financial institutions over the course of their conspiracy.

v. Deposits into LICHTENSTEIN's and MORGAN's Accounts at VCE 8

40. According to records provided by VCE 8, two accounts at VCE 8 were owned by LICHTENSTEIN, with one in the name of Demandpath ("Lichtenstein's VCE 8 Account 1") and the other in the name of Endpass ("Lichtenstein's VCE 8 Account 2").

41. The records also showed that LICHTENSTEIN represented via email to VCE 8 that he would be using his VCE 8 account to trade virtual currency that he had acquired as a result of his early investment in BTC and altcoins.[27] In reality, according to VCE 8 records and the blockchain, LICHTENSTEIN's VCE 8 Account 1 received the bulk of its funds directly, and indirectly, from the above-referenced VCE 4 accounts.

42. A review of Demandpath's public website revealed that it consists of approximately two sentences of text about the company, an address in New York, and a contact email account. No other public information about Demandpath could be located.

43. According to records provided by a USFI ("USFI 5"), from approximately November 2018 to August 2019, Endpass had a bank account at USFI 5. These records also showed that LICHTENSTEIN and MORGAN had multiple other business accounts at USFI 5.

44. LICHTENSTEIN and MORGAN provided statements and certain documentation to support opening their USF1 5 accounts, representing that customer payments into the account would be processed by a U.S.-based financial services and software-as-a-service company. A review of the transactions in and out of this account, as supported by the business records and the BTC blockchain, indicate that the purported Endpass account was not used for this purpose at all, as it conducted zero transactions via this financial services business. Rather, for the period of March 2018 to October 2020, the bulk of the funds received were from approximately five wires from VCE 8, totaling over $758,000. The only other significant deposit to the account was an

[27] Altcoin is a term used for virtual currency other than BTC.

approximately $11,000 U.S. Small Business Administration Paycheck Protection Program (PPP) loan advance provided in response to the COVID-19 crisis.

vi. Following the Flow of Funds from Cluster[28] 36B6mu to Accounts Owned by LICHTENSTEIN and MORGAN

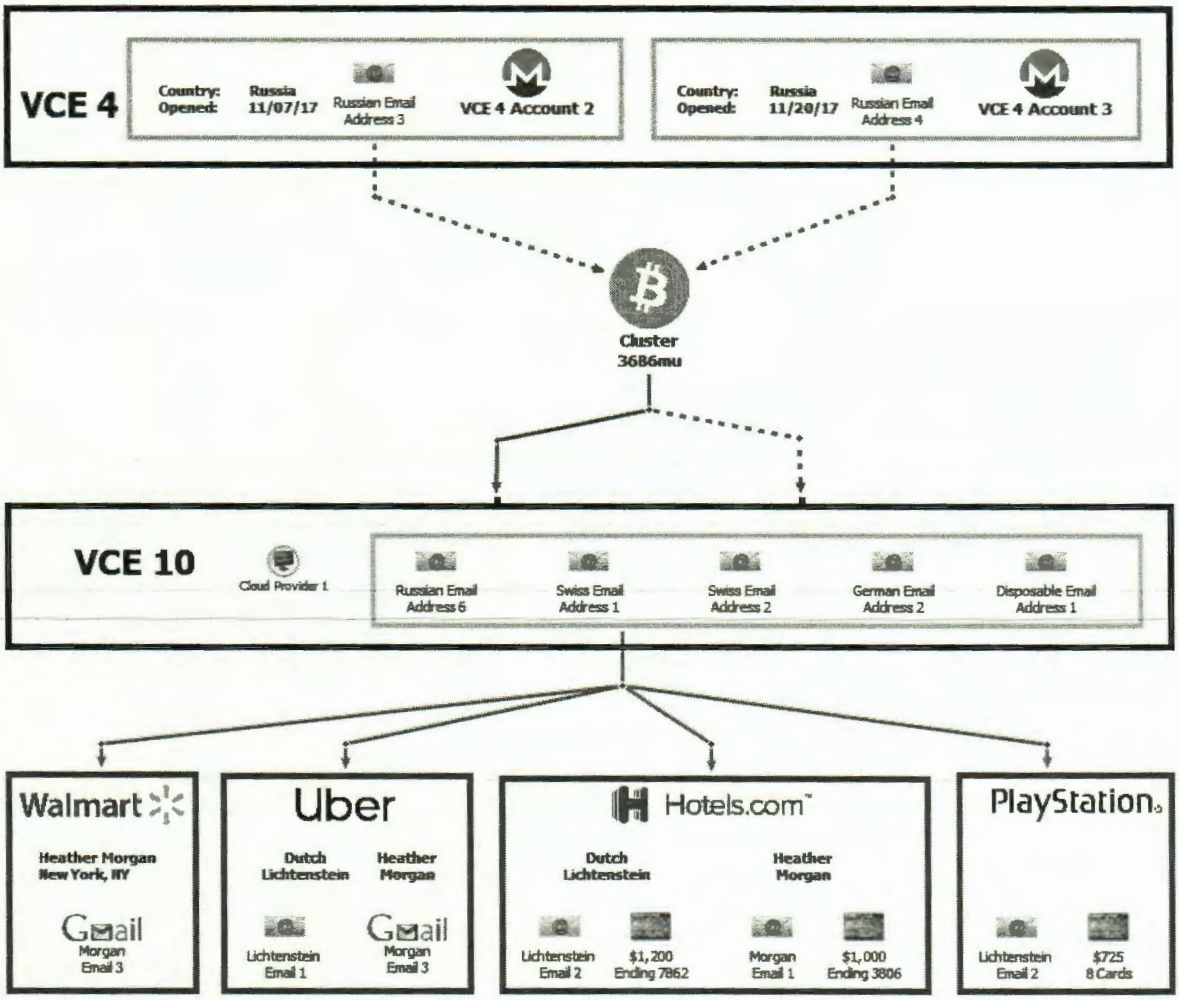
45. While conducting detailed blockchain analysis, investigators observed the importance of a specific BTC cluster ("Cluster 36B6mu"). This cluster was frequently used as an intermediary cluster between VCEs withdrawing BTC and VCE accounts owned by LICHTENSTEIN and MORGAN. This is shown in more detail below.

46. From on or about February 11, 2019, to December 14, 2020, approximately 177.116 BTC flowed through Cluster 36B6mu. A major funding source of Cluster 36B6mu was VCE 4 Account 2 and VCE 4 Account 3. The destination of BTC sent by Cluster 36B6mu was ultimately accounts owned by LICHTENSTEIN and MORGAN.

47. On or about May 3, 2020, Cluster 36B6mu sent approximately 0.057 BTC directly to VCE 10. VCE 10 is a business that sells prepaid gift cards in exchange for BTC. Records from VCE 10 showed that this specific transaction was for the purchase of a $500 gift card to Walmart from an account registered with an email address hosted by a provider in Russia and conducted via an IP address resolving to a New York City-based cloud service provider ("Cloud Provider 1"). Records from Cloud Provider 1 showed that the IP address was leased by an account in the name of LICHTENSTEIN and tied to Lichtenstein Email 1.

48. The chart below shows the movement of funds from Cluster 36B6mu to VCE 10 and the purchase of the $500 gift card:

[28] A cluster is a grouping of addresses believed to be contained within a single wallet.



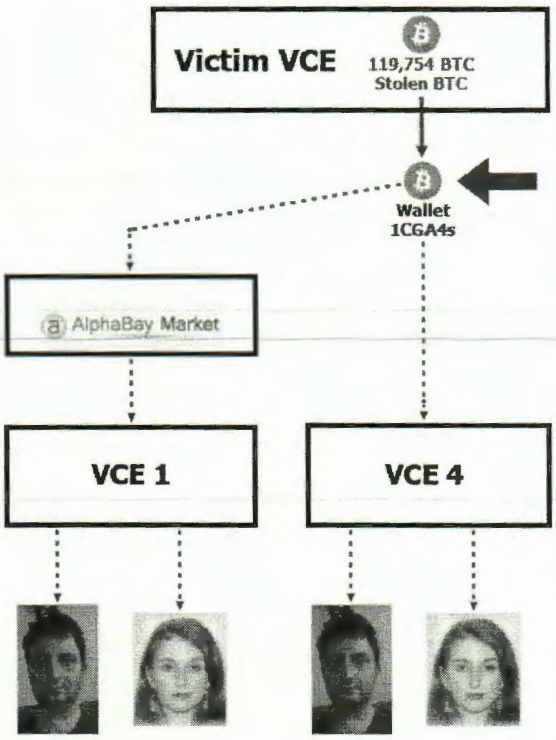
49. Records showed that portions of the $500 gift card were then redeemed through three transactions for personal items via the Walmart iPhone application. Each of the three redemptions were conducted online under MORGAN's name, using one of MORGAN's email addresses, and providing MORGAN and LICHTENSTEIN's home address for delivery.

50. Cluster 36B6mu directly sent BTC to VCE 10 for the purchase of prepaid gift cards on approximately 16 occasions, including the one described above. Although the VCE 10 accounts were registered with multiple email addresses, all but one transaction was conducted from the same Cloud Provider IP address owned by LICHTENSTEIN.

III. LICHTENSTEIN's Cloud Storage Account

51. Lichtenstein Email 2 was held at a U.S.-based provider that offered email as well as cloud storage services, among other products. In 2021, agents obtained a copy of the contents of the cloud storage account pursuant to a search warrant. Upon reviewing the contents of the account, agents confirmed that the account was used by LICHTENSTEIN. However, a significant portion of the files were encrypted.

52. On or about January 31, 2022, law enforcement was able to decrypt several key files contained within the account. Most notably, the account contained a file listing all of the addresses within Wallet 1CGA4s and their corresponding private keys. Using this information, law enforcement seized the remaining contents of the wallet, totaling approximately 94,636 BTC, presently worth $3.629 billion, as described above. The chart below singles out, with an arrow, Wallet 1CGA4s:



53. LICHTENSTEIN's cloud storage account also contained the account spreadsheet, discussed in the preceding subsections, detailing the log-in information and status of accounts at numerous VCEs, including a notation of which accounts had been frozen or emptied. As explained above, many of these accounts received stolen funds from Victim VCE.

54. Furthermore, LICHTENSTEIN's cloud storage account also contained a folder named "personas." The "personas" folder contained biographical information and identification documents for numerous individuals. The account also included a text file named "passport_ideas" that included links to different darknet vendor accounts that appeared to be offering passports or identification cards for sale.

55. LICHTENSTEIN's cloud storage account contained a folder holding data files for numerous financial institutions with notes that appear to be reconnaissance of potential laundering avenues. For example, a document for Alfa-Bank describes the bank as a "sketchy Russian oligarch bank" and includes notes about log-in procedures.

IV. LICHTENSTEIN and MORGAN's Actions Obstructed Lawful Functions of FinCEN

56. Based on my training and experience, I am aware that the Bank Secrecy Act (BSA) and its implementing regulations require financial institutions, including VCEs, to establish and maintain programs designed to detect and report suspicious activity, and to maintain certain records "where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 31 U.S.C. § 5311. Among other things, VCE and USFIs are required to comply with regulations requiring them "to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1). Specifically, VCEs and USFIs must "file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation." 31 C.F.R. § 1022.320(a)(1). This requirement may be triggered by transactions believed to involve funds derived from illegal activity or intended to hide or disguise funds or assets derived from illegal activity; transactions that serve no business or apparent lawful purpose, and for which the VCE knows of no reasonable explanation after examining the available facts; or transactions that involve the use of the virtual currency exchange to facilitate criminal activity. *Id.* § 1022.320(a)(2)(i), (iii), (iv). Such reports are commonly known as Suspicious Activity Reports ("SARs").

57. The Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of Treasury, is responsible for the implementation, administration, and enforcement of the Bank Secrecy Act. FinCEN's mission is "to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence." FinCEN is headquartered in Washington, D.C.

58. At the time of the relevant activity described above, USFI 5, VCE 1, VCE 4, VCE 5, VCE 7, VCE 8, VCE 9, and VCE 10 were financial institutions doing business in the United States, subject to the Bank Secrecy Act, and were registered with FinCEN. According to records provided by two VCEs, LICHTENSTEIN expressed his knowledge of these regulations in communications with the VCEs, telling one VCE that he chose to do business with it "to ensure that I am trading fiat in a regulated, compliant exchange," and telling another VCE that his sources of funds included "other regulated cryptocurrency exchanges." MORGAN similarly conveyed familiarity with these regulations, advising VCE 7 that, because SalesFolk was not a financial institution managing customers' funds, "we haven't been doing any KYC on [SalesFolk customers]."

59. During the course of the conspiracy, LICHTENSTEIN and MORGAN repeatedly provided false information to and deceived the VCEs and other financial institutions regarding the source of their funds and the nature of their transactions. One purpose of these deceptions was to frustrate the VCEs' due diligence efforts and thereby prevent the transmission of SARs mandated under the Bank Secrecy Act to FinCEN and the U.S. Department of the Treasury in Washington, D.C. A sample of such deceptions are included in the paragraphs above.

V. Conclusion

60. Based on the foregoing, your affiant submits that there is probable cause to believe that ILYA "DUTCH" LICHTENSTEIN and HEATHER MORGAN violated 18 U.S.C. § 1956(h), which makes it a crime in relevant part to conspire to conduct or attempt to conduct a financial transaction involving the proceeds of specified unlawful activity, knowing that the property involved in the financial transaction represents the proceeds of some form of unlawful activity, and knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity. For purposes of this section, specified unlawful activity includes wire fraud, in violation of 18 U.S.C. § 1343, and computer fraud and abuse, in violation of 18 U.S.C. § 1030.

61. Your affiant submits there is also probable cause to believe that ILYA "DUTCH" LICHTENSTEIN and HEATHER MORGAN violated 18 U.S.C. § 371, which makes it a crime in relevant part for two or more persons to conspire to defraud the United States, or any agency thereof, in any manner or for any purpose, and to do any act to effect the object of the conspiracy.

Christopher Janczewski
Special Agent
IRS-Criminal Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 7th day of February 2022.

Robin M. Meriweather
2022.02.07 11:11:48
-05'00'

ROBIN M. MERIWEATHER
U.S. MAGISTRATE JUDGE